UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/043,654	01/10/2002	Nelson Waldo Bunker V.	500939.000004	7438

37141 7590 08/24/2005

FORTKORT GRETHER + KELTON LLP
8911 N. CAPITAL OF TEXAS HWY.
SUITE 3200
AUSTIN, TX 78759

EXAMINER	
ELMORE, JOHN E	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 08/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/043,654	BUNKER V. ET AL.	
	Examiner	Art Unit	
	John Elmore	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-102* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-60,62,64-66,68,70-72,74 and 76-102* is/are rejected.

7)☒ Claim(s) *61, 63, 67, 69, 73 and 75* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-102 have been examined.

Claim Objections

2. **Claims 69 and 74-75 are objected** to because of the following informalities:

The term "apparatus" in claim 69 (line 1) presumably should read "method".

The term "method" in claim 74 (line 1) presumably should read "computer program product".

The term "apparatus" in claim 74 (line 1) presumably should read "computer program product".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. **Claims 5, 6, 17, 18, 77-79, 81, 85, 92, 94, 96, 98, 100 and 102 are rejected under 35 U.S.C. 112, second paragraph**, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "security obstacle" in claims 5 (line 2), 6 (line 1), 17 (line 2), 18 (line 1), 77 (lines 1-2), 81 (lines 1-2), 85 (line 2), 92 (line 3), 94 (line 2), 96 (line 2), 98 (line 2),

100 (lines 1-2) and 102 (lines 1-2) is a relative term which renders the claim indefinite. The term "security obstacle" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. It is uncertain whether the term refers to a network security vulnerability as widely understood in the art. In the interest of compact prosecution, the limitations containing the term "security obstacle" subsequently are ignored.

The term "session establishability information" in claims 6 (line 2), 18 (line 2) is a relative term which renders the claim indefinite. The term " session establishability information" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. It is uncertain whether the term refers to information that describes the communication session of a device over a network as widely understood in the art. In the interest of compact prosecution, the limitations containing the term "session establishability information" subsequently are ignored.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. **Claims 1-60, 62, 64-66, 68, 70-72 and 74 are rejected under 35 U.S.C. 103(a)** as being anticipated by Gleichauf et al. (US 6,301,668), hereafter Gleichauf I, and Gleichauf et al. (US 6,324,656), incorporated by reference, hereafter Gleichauf II.

Regarding claim 1, Gleichauf I and II disclose a network security testing apparatus comprising:

a first tester that is adapted to communicably couple to a system under test (Gleichauf I: a first tester employing one of a plurality of tools of the scan engine 22; Gleichauf II: a first NVA engine coupled to network; col. 3, lines 41-67);

wherein said first tester is adapted to perform a plurality of tests on the system under test (Gleichauf II: Fig. 3A; the NVA engine performs the tests of preliminary analysis and active analysis; col. 6, lines 8-21);

wherein the plurality of tests includes a first test (preliminary analysis) and a second test (active exploits analysis), each of which is adapted to return system environment information regarding the system under test (Gleichauf II: each test gathers information about network devices, services, or vulnerabilities and returns it to port database 22; col. 6, lines 22-23);

wherein the first test is executed before the second test (Gleichauf II: preliminary analysis 94 performed before active exploits analysis 98; Fig. 3A); and

wherein the first test differs from the second test in that the second test is more specific to the system under test based on information gained from the first test (Gleichauf II: active exploits analysis, the second test, is based on particular information received from the preliminary analysis, the first test; col. 8, lines 12-17).

Regarding claim 2, Gleichauf I and II teach all the limitations of claim 1, and further teach that no tests are performed on the system under test after the first test and before the second test, wherein the time period between the first test and the second test can be negligible (Gleichauf II: the second test, active exploits 98, immediately follows the first test, preliminary analysis 94, as host nudge 96 is omitted as optional, and the delay is negligible because active exploits runs in real-time and proceeds as soon as data from first test is available; Fig. 3A; col. 6, lines 8-10; col. 8, lines 8-19).

Regarding claim 3, Gleichauf I and II teach all the limitations of claim 1, and further teach that the second test is based at least partially upon system environment information detected by the first test (Gleichauf II: col. 8, lines 12-17).

Regarding claim 4, Gleichauf I and II teach all the limitations of claim 3, and further teach that the system environment information includes information regarding network connectivity from the first tester to the system under test (Gleichauf II: information from first test is stored in port database 22 and identifies, for example, what ports are active on workstations connected to the network; col. 4, lines 20-30 and 40-42).

Regarding claims 5 and 6, these claims are rejected on the same basis as claim 3, as the distinguishing limitations have been ignored via the 35 U.S.C. 112 second paragraph rejections above.

Regarding claim 7, Gleichauf I and II teach all the limitations of claim 3, and further teach that an apparatus comprising:

a second tester that is adapted to communicably couple to a system under test (Gleichauf I: a second tester of the scan engine 22; Gleichauf II: a second NVA engine coupled to network; col. 3, lines 41-67);

wherein the first test (preliminary analysis) is executed by said first tester (first NVA engine);

wherein determination of whether the second test (either an active exploits analysis test or a repeat preliminary analysis test) is executed by said first tester or by said second tester is made based at least partially upon the system environment information (Gleichauf II: iterative process determines whether second test is conducted as an active exploits test by second NVA engine or as a further preliminary analysis test by first NVA engine; col. 7, lines 55-61).

Regarding claim 8, Gleichauf I and II teach all the limitations of claim 3, and further teach that the second test includes execution of a test tool selected from a plurality of test tools based at least partially upon the system environment information (Gleichauf II: a plurality of tests is noted by the provision of at least two examples, and it is inherent that the selection of a test tool among a plurality of test tools stems from the selection of a test from a plurality of tests, wherein the tests differ from one another as to require different tools; col. 6, lines 15-18).

Regarding claim 9, Gleichauf I and II teach all the limitations of claim 3, and further teach that said first tester is adapted to execute an additional test of the plurality of tests if said first tester has not yet definitely gathered all possible system environment information about the system under test, in light of the plurality of tests (Gleichauf II:

iterative process determines whether an additional test is conducted as further preliminary analysis by first NVA engine based upon whether first NVA engine has gathered all possible system environment information; col. 7, lines 55-61).

Regarding claim 10, Gleichauf I and II teach all the limitations of claim 2, and further teach that the second test is based at least partially upon system environment information detected by the first test (Gleichauf II: col. 8, lines 12-17).

Regarding claim 11, Gleichauf I and II teach all the limitations of claim 7, and further teach that the second test includes execution of a test tool selected from a plurality of test tools based at least partially upon the system environment information (Gleichauf II: a plurality of tests is noted by the provision of at least two examples, and it is inherent that the selection of a test tool among a plurality of test tools stems from the selection of a test from a plurality of tests, wherein the tests differ from one another as to require different tools; col. 6, lines 15-18).

Regarding claim 12, Gleichauf I and II teach all the limitations of claim 7, and further teach that said first tester is adapted to execute an additional test of the plurality of tests if said first tester has not yet definitely gathered all possible system environment information about the system under test, in light of the plurality of tests (Gleichauf II: iterative process determines whether an additional test is conducted as further preliminary analysis by first NVA engine based upon whether first NVA engine has gathered all possible system environment information; col. 7, lines 55-61).

Regarding claims 13-24 and 25-36, these are a method and computer-program-product versions, respectively, of the claimed apparatus above (claims 1-12). Therefore, for reasons applied above, such a claims also is anticipated.

Regarding claim 37, Gleichauf I and II disclose a network security testing apparatus comprising:

a customer profile (Gleichauf I: network map 28; col. 6, lines 5-19; col. 7, line 61);

a plurality of test tools (Gleichauf I: scan engine 22 employs a plurality of test tools; col. 7, lines 45-49; Gleichauf II: Fig. 3A; the NVA engine performs a plurality of tests including preliminary analysis and active analysis, collectively referred to as the analysis phase; col. 4, lines 43-55; col. 6, lines 8-21);

a first tester that is adapted to communicably couple to a system under test (Gleichauf I: a first tester employing one of a plurality of tools of the scan engine 22; Gleichauf II: a first NVA engine coupled to network; col. 3, lines 41-67);

wherein a selected test tool is selected from said plurality of test tools based at least partially upon said customer profile (Gleichauf I: network map 28 created with information normally collected during discovery phase, steps 100, 102 and 104, and testing performed using the network map; Fig. 4; col. 6, lines 15-20; col. 8, lines 1-27; Gleichauf II: preliminary analysis 94 based upon network information gathered during discovery 90; Fig. 3A; col. 5, lines 27-40 and 62-64; col. 5, line 58-col. 6, line 12; col. 6, lines 26-28); and

wherein said first tester is adapted to execute the selected test tool so as to test the system under test (Gleichauf II: a first NVA engine executes preliminary analysis; col. 5, lines 58-61).

Regarding claim 38, Gleichauf I and II teach all the limitations of claim 37, and further teach that said customer profile is determined based at least partially upon an initial mapping (Gleichauf I: network map 28; col. 6, lines 5-20).

Regarding claim 39, Gleichauf I and II teach all the limitations of claim 37, and further teach that the customer profile is based at least partially on information provided by a third party (Gleichauf I: network map 28 based at least partially on information provided by third party mapping service; col. 6, lines 15-20; col. 8, lines 24-27).

Regarding claim 40, Gleichauf I and II teach all the limitations of claim 37, and further teach that the customer profile is at least partially produced by the method of claim 24 (Gleichauf II: discovery phase is an iterative process, wherein additional tests are conducted until the system environment information is collected into a port database 22, which forms the basis for the network map; col. 7, lines 27-40 and 55-62).

Regarding claim 41, Gleichauf I and II teach all the limitations of claim 37, and further teach an apparatus comprising:

a second tester that is adapted to communicably couple to the system under test (Gleichauf I: a second tester of the scan engine 22; Gleichauf II: a second NVA engine coupled to network; col. 3, lines 41-67);

wherein determination of whether the first tester or the second tester executes the selected test tool is based at least partially upon said customer profile (Gleichauf II:

iterative process determines whether second test is conducted as an active exploits test 98 by second NVA engine or as a further preliminary analysis test 94 by first NVA engine, wherein determination is based on information in port database 22/network map; Fig. 3A; col. 5, lines 36-40; col. 6, lines 8-12 and 34-37; col. 7, lines 55-61).

Regarding claim 42, Gleichauf I and II teach all the limitations of claim 37, and further teach that the customer profile is based at least partially on information provided by a third party (Gleichauf I: network map 28 based at least partially on information provided by third party mapping service; col. 6, lines 15-20; col. 8, lines 24-27).

Regarding claim 43, Gleichauf I and II teach all the limitations of claim 42, and further teach that the customer profile is at least partially produced by the method of claim 24 (Gleichauf II: discovery phase is an iterative process, wherein additional tests are conducted until the system environment information is collected into a port database 22, which forms the basis for the network map; col. 7, lines 27-40 and 55-62).

Regarding claims 44-50 and 51-57, these are a method and computer-program-product versions, respectively, of the claimed apparatus above (claims 37-43). Therefore, for reasons applied above, such a claims also is anticipated.

Regarding claim 58, Gleichauf I and II teach an apparatus comprising:

a plurality of testers (Gleichauf II: plurality of NVA engines; col. 3, lines 57-67);

a customer profile (Gleichauf I: network map 28; col. 6, lines 5-19; col. 7, line 61);

wherein each of said plurality of testers is adapted to communicably couple to a system under test (Gleichauf II: NVA engines each couple to the network being tested; col. 3, lines 43-50 and 57-63); and

wherein a test of the system under test is performed by a selected tester of said plurality of testers, the selected tester being selected from said plurality of testers based at least partially upon said customer profile (Gleichauf II: iterative process determines whether second test is conducted as an active exploits test 98 by second NVA engine or as a further preliminary analysis test 94 by first NVA engine, wherein determination is based on information in port database 22/network map; Fig. 3A; col. 5, lines 36-40; col. 6, lines 8-12 and 34-37; col. 7, lines 55-61).

Regarding claim 59, Gleichauf I and II teach all the limitations of claim 58, and further teach that said customer profile is determined based at least partially upon an initial mapping (Gleichauf I: network map 28; col. 6, lines 5-20).

Regarding claim 60, Gleichauf I and II teach all the limitations of claim 58, and further teach that the customer profile is at least partially produced by the method of claim 24 (Gleichauf II: discovery phase is an iterative process, wherein additional tests are conducted until the system environment information is collected into a port database 22, which forms the basis for the network map; col. 7, lines 27-40 and 55-62).

Regarding claim 62, Gleichauf I and II teach all the limitations of claim 58, and further teach an apparatus:

wherein each tester of said plurality of testers has at least one quality of communicable coupling to the system under test (Gleichauf II: location of coupled NVA engine impacts access to devices on network; col. 3, lines 64-67); and

wherein the selected tester is selected from said plurality of testers based at least partially on the selected tester's quality of communicable coupling (Gleichauf II: it is

inherent that certain NVA engines will be selected where they provide exclusive access to certain devices on a network; col. 3, lines 64-67).

Regarding claims 64-66, 68, 70-72 and 74, these are a computer-program-product and method versions, respectively, of the claimed apparatus above (claims 58-60 and 62). Therefore, for reasons applied above, such claims also are anticipated.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 76-87 and 91-101 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Gleichauf I and II.

Regarding claim 76, Gleichauf I and II teach a network security testing apparatus comprising a first tester that is adapted to communicably couple to a system under test, wherein said first tester is adapted to perform a test on the system under test (Gleichauf I: a first tester employing one of a plurality of tools of the scan engine 22; Gleichauf II: a first NVA engine coupled to network; col. 3, lines 41-67; col. 6, lines 8-21). But Gleichauf I and II do not explain an apparatus wherein said first tester is adapted to make a first attempt to communicably couple to the system under test before the test; wherein said first tester is adapted to make a second attempt to communicably couple to the system under test after the test; and wherein the combination of success

of the first attempt and failure of the second attempt are interpreted as detection of the test by the system under test.

However, it is widely known in the art that security testing involves multiple attempts by a tester to administer a test and that detection of the test is generally suspected as a result of the failure in the attempt of the testing device to couple to a network subsequent to the successful administration of the test upon the network using the same configuration. The Examiner takes official notice that one of ordinary skill in the art would recognize the detection of a test by the system under test as a plausible interpretation of the pattern of results where a second attempt of a tester to couple to a network fails after a first attempt has been successful and the test administered.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to provide an apparatus wherein said first tester is adapted to make a first attempt to communicably couple to the system under test before the test; wherein said first tester is adapted to make a second attempt to communicably couple to the system under test after the test; and wherein the combination of success of the first attempt and failure of the second attempt are interpreted as detection of the test by the system under test, for the motivation of providing a plausible interpretation for the pattern of results from the first and second attempts of the tester to couple to the system.

Regarding claim 77, this claim is rejected on the same basis as claim 76, as the distinguishing limitations have been ignored via the 35 U.S.C. 112 second paragraph rejections above.

Regarding claim 78, Gleichauf I and II teach all the limitations of claim 77, but do not explain an apparatus wherein the first attempt is made using a first originating P address; wherein the second attempt is made using a second originating IP address that is essentially the same as the first originating IP address; wherein a third attempt to communicably couple to the system under test is made using a wherein the combination of success of the first attempt, failure of the second attempt, and success of the third attempt is interpreted as a possibility including the detection; and wherein the combination of success of the first attempt, failure of the second attempt, and failure of the third attempt is interpreted as a possibility including: a network connectivity problem between the first tester and the system under test; and the detection.

However, it is widely known in the art that security testing involves multiple attempts by a tester to administer a test and that detection of the test is generally suspected as a result of the failure in the attempt of the testing device to couple to a network subsequent to the successful administration of the test upon the network using the same configuration, including essentially the same originating IP address. The Examiner takes official notice that one of ordinary skill in the art would recognize the detection of a test by the system under test as a plausible interpretation of the pattern of results where a second attempt of the tester to couple to a network using a second originating IP address that is essentially equal to a first originating IP address fails after a first attempt using the first originating IP address has been successful and the test administered. One of ordinary skill in the art would also recognize that this interpretation would be supported upon the success of a third attempt of the tester to

couple to the network using a third originating IP address different from the second originating IP address because the third attempt proves that the tester suffers no connectivity problem. Further, one of ordinary skill in art would recognize that the interpretation of the first two attempts would be undermined upon the failure of a third attempt of the tester to couple to the network using a third originating IP address different from the second originating IP address because the third attempt suggests the possibility that the tester suffers a connectivity problem, as the third attempt would be expected to following the same pattern starting with the first attempt. As such, one of ordinary skill in the art would recognize the existence of two plausible interpretations of a series of failed attempts to couple to the system using different originating IP addresses: a network connectivity problem and a detection.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to provide an apparatus wherein the first attempt is made using a first originating P address; wherein the second attempt is made using a second originating IP address that is essentially the same as the first originating IP address; wherein a third attempt to communicably couple to the system under test is made using a wherein the combination of success of the first attempt, failure of the second attempt, and success of the third attempt is interpreted as a possibility including the detection; and wherein the combination of success of the first attempt, failure of the second attempt, and failure of the third attempt is interpreted as a possibility including: a network connectivity problem between the first tester and the system under test; and the

detection, for the motivation of providing a plausible interpretation for the pattern of results from the first, second, and third attempts of the tester to couple to the system.

Regarding claim 79, this claim is rejected on the same basis as claim 78, noting that for claim 76 the distinguishing limitations have been ignored via the 35 U.S.C. 112 second paragraph rejections above.

. **Regarding claims 80-87,** these are a method and computer-program-product versions of the claimed apparatus above (claims 76-78). Therefore, for reasons applied above, such claims also would have been obvious.

Regarding claim 91, Gleichauf I and II disclose a network security testing apparatus comprising:

a tester that is communicably coupled to a system under test, wherein said tester is adapted to test the system under test (signature engine 26; col. 6, lines 37-40);

wherein said tester is adapted to execute a first test tool to test the system under test (a first attack signature from among a plurality of attack signatures 30);

wherein said tester is adapted to execute a second test tool to test the system under test (a second attack signature from among a plurality of attack signatures 30).

But Gleichauf I and II do not explicitly explain that a time period of selected length is interposed between the execution of the first test tool and the execution of the second test tool during which said tester does not test the system under test.

However, Gleichauf I and II teach that test tools pertaining to attack signatures are assigned priorities for execution by the priority engine 32 in a prioritized attack signature list 150 (Gleichauf I: col. 6, lines 59-62) and that the execution of tests on the

list is suspended in the order of priority by determination of the priority engine (Gleichauf I: col. 9, lines 33-38 and 39-49). The Examiner takes official notice that one of ordinary skill in the art would recognize that where a first test tool and a second test tool differ in priority such that the priority engine determines that the execution of the second test tool is suspended, a time period of selected length is interposed between the execution of the first test tool and the second test tool wherein no testing is performed by the tester.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to provide that a time period of selected length is interposed between the execution of the first test tool and the execution of the second test tool during which said tester does not test the system under test for the motivation of suspending testing where the priority engine determines that it is necessary to do so.

Regarding claim 92, Gleichauf I and II teach all the limitations of claim 58, and further teach that the selected length is of random length (it is inherent that the demand on system resources which would require the priority engine to suspend execution of a test tool is randomly determined by the interaction of the myriad of devices utilizing the network; hence, the time period of the suspension is randomly determined). Therefore, for reasons applied above, such claims also would have been obvious.

Regarding claims 93-94 and 95-96, these are a method and computer-program-product versions of the claimed apparatus above (claims 91 and 92). Therefore, for reasons applied above, such claims also would have been obvious.

Regarding claim 97, Gleichauf I and II disclose a network security testing apparatus comprising:

a plurality of testers (Gleichauf I: protocol engine 24 and signature engine 26; col. 5, lines 43-51);

a plurality of test tools (Gleichauf I: a plurality of protocol analyses; col. 6, lines 25-26; attack signatures 30; col. 6, lines 39-42);

wherein each of said plurality of testers is adapted to communicably couple to a system under test (Gleichauf I: col. 5, lines 43-51).

But Gleichauf I and II do not explain that a random one of said plurality of test tools is executed by a random one of said plurality of testers, the random one of said plurality of test tools being executed so as to target the system under test, whereby the system under test is tested.

However, it is widely known in the art to administer security testing by selecting test tools and tests randomly from a plurality, as this method simulates random attacks on the system while also being a simple and efficient. The Examiner takes official notice that one of ordinary skill in the art would recognize that where there exists a plurality of testers and a plurality of test tools from which to select, and where the priority engine determines that there exists equal priority in the order of execution of the plurality of testers and plurality of test tools or that system resources are sufficient to obviate the need to prioritize test execution, random selection of one among the plurality of testers and one among the plurality of test tools is warranted.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to provide that a random one of said plurality of test tools is executed by a random one of said plurality of testers, the random one of said plurality of test tools being executed so as to target the system under test, whereby the system under test is tested for the motivation of utilizing a simple and efficient means of determining which tester and test tool to execute.

Regarding claim 98, this claim is rejected on the same basis as claim 97, as the distinguishing limitations have been ignored via the 35 U.S.C. 112 second paragraph rejections above.

. **Regarding claims 99 and 101,** these are a method and computer-program-product versions of the claimed apparatus above (claims 97). Therefore, for reasons applied above, such claims also would have been obvious.

9. **Claims 88-90 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Gleichauf I and II in view of Srinivasan ("Binding Protocols for ONC RPC Version 2", Network Working Group RFC 1833, August 1995).

Regarding claim 88, Gleichauf I and II disclose a network security testing apparatus comprising:

a tester (Gleichauf I: network security system 20);

a test tool (Gleichauf I: scan engine 22);

wherein said tester is adapted to be communicably coupled to a system under test (Gleichauf I: col. 5, lines 43-44); and

wherein said tester is adapted to test the system under test by execution of said test tool (Gleichauf I: col. 5, lines 43-51).

But Gleichauf I and II do not explain an application programming interface (API), wherein said API is adapted to interface between said tester and said test tool, such that said test tool may be executed by said tester even if the outputs of said tester do not directly correspond to the inputs of said test tool, and such that said test tool may be executed by said tester even if the inputs of said tester do not directly correspond to the outputs of said test tool.

However, Gleichauf I and II teaches that the test tool (scan engine) runs on a Sun based workstation and is operable remotely from the tester (col. 3, lines 16-32). As it is widely known in the art that remote programs are called using an API known as a Remote Procedure Call (RPC), the Examiner takes official notice that one of ordinary skill in the art would recognize that remote operation of a software program is accomplished on Sun based workstations using the Remote Procedure Call (RPC) API adopted by Sun Microsystems, namely ONC Binding Protocols for RPC version 3. And Srinivasan teaches the ONC Binding Protocols for RPC version 3 wherein calling a remote program requires providing a RPC program number and version for the purpose of providing the RPC services with the information it needs to identify the remote program using its lookup service. It follows that where the tester uses a RPC API to call a remote test program, the outputs from the tester will include a RPC program number and a RPC program version, whereas the tester calling a local test program would not include this information in its outputs.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to provide for an application programming interface (API), wherein said API is adapted to interface between said tester and said test tool, such that said test tool may be executed by said tester even if the outputs of said tester do not directly correspond to the inputs of said test tool, and such that said test tool may be executed by said tester even if the inputs of said tester do not directly correspond to the outputs of said test tool. One would be motivated to do so for the purpose of remotely operating the test tool.

. **Regarding claims 89 and 90,** these are a method and computer-program-product versions of the claimed apparatus above (claim 88). Therefore, for reasons applied above, such claims also would have been obvious.

Allowable Subject Matter

10. **Claims 61, 63, 67, 69, 73 and 75 are objected to** as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Regarding claims 61, 67 and 73, the closest prior art, Gleichauf I and II, does not explain selecting a tester from the plurality of testers based at least partially on optimizing the load balance characteristic.

While load balancing is well known in the art as a method for selecting a server from among a plurality of homogenous servers for the purpose of optimizing network operation, Gleichauf I and II do not explain that the plurality of testers are homogenous.

Gleichauf II teaches a plurality of testers (NVA engines running on servers) that are each coupled to different segments of the network such that each has different access to devices on the network (col. 3, lines 57-67). This configuration implies an inhomogeneous plurality of testers from which to select because the service provided by each tester differs in regard to the information collected from the devices accessible to it even where the test is the same as provided by another tester in the plurality. Hence, as each tester offers a unique service in regard to the application of its test to a particular location, there exists no rationale for the employment of load balancing as a determining factor in selecting a tester. And it would not seem obvious to one of ordinary skill in the art to provide such selection based on load balancing because the prior art makes no suggestion to form a plurality of homogenous testers from which to select, as defined by adding a second tester within the same network segment of a first tester having access to the same devices and offering the same test.

Regarding claims 63, 69 and 75, the closest prior art, Gleichauf I and II, does not explain selecting a tester from a plurality of testers based on the quality of communicable coupling wherein the coupling includes cost per bit, absolute speed, and geographical proximity of the selected tester to the system under test.

While Gleichauf II teaches a plurality of testers (NVA engines running on servers) that are each coupled to different segments of the network, such that each tester represents a different geographical proximity to the system under test (col. 3, lines 57-67), the selection of a tester is based on its accessibility to devices rather than its geographical proximity, which do not necessarily equate to the same thing. The prior

art makes no reference to the selection of a tester based on geographical proximity per se. The prior art also makes no reference to the selection of a tester based on the cost per bit or absolute speed of its communication coupling. Therefore, it would not seem obvious to one of ordinary skill in the art to provide for selecting a tester from a plurality of testers based on the quality of communicable coupling wherein the coupling includes cost per bit, absolute speed, and geographical proximity of the selected tester to the system under test because the prior art provides no motivation for selecting between testers on the basis of these qualities of communicable coupling, particularly where there plurality of testers from which to select is inhomogeneous.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John Elmore whose telephone number is 571-272-4224. The examiner can normally be reached on M 10-8, T-Th 9-7.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 571-272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

John Elmore

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100